Aprobado en Consejo Informático 19-3-2013

- OFFICESCAN – Reputación Web

Contexto y situación actual

Actualmente la forma por la que se infectan los equipos puede ocurrir, como norma general, de tres formas distintas:

1. Correos electrónicos con ficheros comprometidos.
2. Dispositivos de almacenamiento externo.
3. Navegando por Internet o a través de enlaces a páginas comprometidas en los correos electrónicos.

Para las dos primeras opciones existe una solución preventiva ya que cualquier antivirus bloquea la ejecución de código malicioso.

En los últimos años, la tercera forma de infección se ha convertido en la vía por excelencia para infectar equipos debido a los agujeros de seguridad (sobre todo en la máquina virtual de Java) y a la facilidad para encontrar víctimas y sin embargo, en la universidad no sé está utilizando ninguna herramienta que actúe de forma preventiva para evitar este tipo de infecciones.

Actualmente, diversas empresas ofrecen servicios de "Reputación web" como remedio para evitar esta vía de infección. Estos servicios consisten en la creación de *"listas negras de URLs"*, confeccionadas a partir de distintas fuentes. En estas listas se incluyen páginas de phishing, scam, distribución de malware, exploits… de forma que cuando el usuario intenta acceder a una de estas páginas, el servicio de reputación web las bloquea y avisa al usuario, impidiendo de esta forma la infección del equipo.

Reputación Web con Trend Micro Office Scan

La tecnología de reputación Web de Trend Micro realiza un seguimiento de la credibilidad de los dominios Web y permite garantizar que las páginas a las que accede el usuario son seguras y no contienen amenazas Web, como malware, spyware o fraudes de phishing que tienen como objetivo engañar al usuario para que proporcione información personal.

Los clientes de OfficeScan pueden hacer uso de los Servicios de Reputación Web.

La lista negra de Trend Micro, permite una gestión manual a través de la consola del antivirus, para añadir páginas a la lista negra, bloqueando su acceso, o para sacar páginas de la lista negra, permitiendo su acceso.

Cuando el antivirus encuentra una página web que está incluida como URL maliciosa o sitio web de phising procede a su bloqueo. El funcionamiento es similar a cuando se bloquea la ejecución de un programa-malware que intenta infectar el pc.

Bloqueo de URL

Cuando un usuario está navegando e intenta acceder a una página que no supera el filtro de reputación web, le aparece la siguiente información, relativa al bloqueo de la URL:

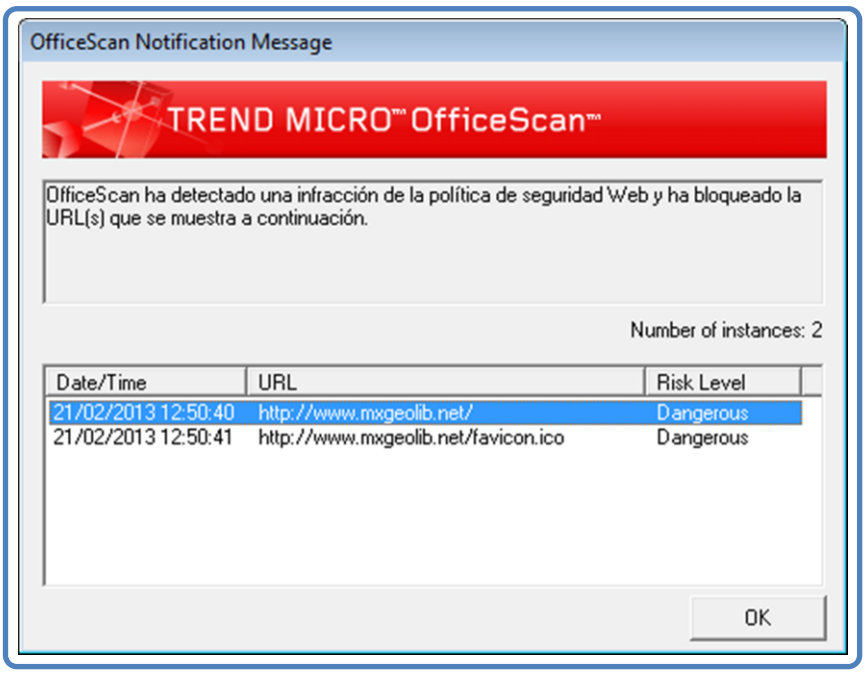

Imagen 1. Notificación del antivirus para un intento de acceso a una página web maliciosa incluida en la lista negra

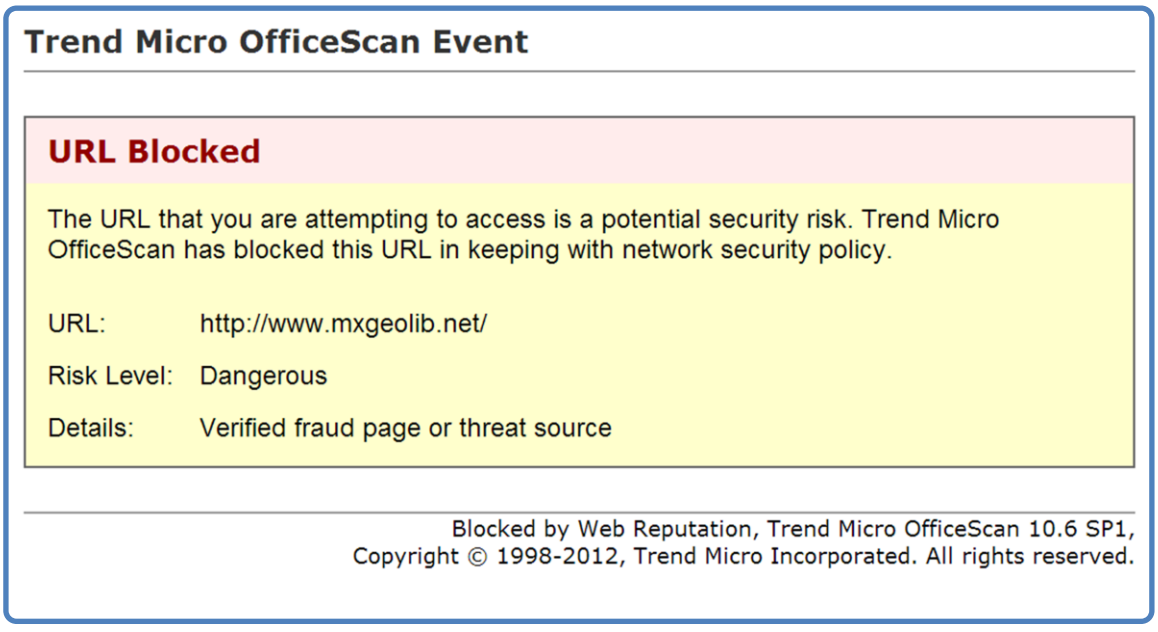

Imagen 2. Notificación de página bloqueada mostrada en el navegador

Niveles de seguridad

Existen 3 niveles de seguridad disponibles para la reputación Web:

- Alto
- Medio
- Bajo

Estos niveles de seguridad determinan si OfficeScan bloqueará el acceso a una página web. Por defecto, se habilitaría el ***nivel de seguridad Bajo*** en el cual OfficeScan únicamente bloqueará aquellas direcciones web (URL) que son amenazas Web conocidas.

NIVEL DE SEGURIDAD	*ELEMENTO BLOQUEADO*
Alto	*URLs maliciosas conocidas*
	Sitios de phising conocidos
	Alta probabilidad de ser URL maliciosas
	Alta probabilidad de ser Sitios de phishing
	Sitios conocidos de spamming
	Comportamientos conocidos con mala reputación
Medio	*URLs desconocidas*
	URLs maliciosas conocidas
	Sitios de phising conocidos
	Alta probabilidad de ser URL maliciosas
	Alta probabilidad de ser Sitios de phishing
Bajo	*URLs maliciosas conocidas*
	Sitios de phising conocidos

Imagen 3. Niveles de seguridad para la Reputación web de Trend Micro

	SAFE Not malware to Trend Micro's knowledge	WARNING With Spamming history or bad reputation behaviors	DANGEROUS High probability that this is malicious or Phishing	HIGHLY DANGEROUS Known Malicious (Spyware, Malware or Phishing)
HIGH	✓			
Medium	✓	✓		
Low	✓	✓	✓	

Imagen 4. Funcionamiento de la Reputación web de Trend

NOTA: Si se aumenta el nivel de seguridad, la tasa de detección de amenazas Web aumenta, pero también la posibilidad de falsos positivos, por lo que inicialmente se descarta la opción de aumentar dicho nivel de seguridad.

Gestión de manual de sitios web por parte la UC3M

La consola Central de Officescan, permite realizar una gestión manual de la lista negra, de forma se pueden agregar sitios web que se consideren seguros para la universidad pero formen parte de la lista negra de Trend Micro, de manera que cuando el usuario intente acceder a ellos, en vez de bloquear la página web, le permita el acceso. De la misma manera, se pueden añadir sitios web que se consideren peligrosos pero que no formen parte de la lista negra, de forma que cuando el usuario intente acceder a dichas páginas se bloqueará el acceso, aunque no formen parte de la lista negra de Trend Micro.

Todas estas acciones tendrían que ser realizadas por los Administradores de la consola, previa petición de los usuarios para, o bien permitir, o bien bloquear un sitio web concreto.

Procedimiento para solicitar un bloqueo/desbloqueo

Para solicitar el bloqueo/desbloqueo de una página web, será necesario comunicarlo como cualquier incidencia a través de http://hidra.uc3m.es o el CASO.

Registro de reputación web en Consola de Administración

La información que se almacena en el servidor de Officescan es exclusivamente de URLs bloqueadas e incluye los siguientes datos:

Date/Time	*Computer*	*URL*	*Risk Level*
21/02/2013 12:50	PC-XX-ZZZ	http://www.mxgeolib.net/	Dangerous

Imagen 5. Registro de reputación web en Consola de Administración

Ejemplos

Los ejemplos que se muestran a continuación, son problemas reales, que han ocurrido en los últimos meses, algunos ya solucionados y otros que continúan representando una amenaza. Todos estos casos, no constituyen una amenaza, cuando está activado el servicio de Reputación web, debido a que, es el propio antivirus del usuario el que bloquea el acceso a páginas comprometidas, de la misma manera que el servicio "Realtime Scan" evita la ejecución de ficheros y programas maliciosos.

Ejemplo 1: Página web NBC con código malicioso incrustado:

En la página web de la NBC, incrustaron código malicioso que se ejecutaba e infectaba el equipo que visitaba esa dirección web. TODO el mundo que accedió a dicha página (con SO Windows) se infectó con un troyano bancario, sin que el usuario se enterase. Con la reputación web activada, se bloquea el acceso a la página comprometida, que no al dominio, evitando la infección

Más información en:

- http://unaaldia.hispasec.com/2013/02/fines-y-medios-ahora-la-nbc.html

Ejemplo 2: Página web que utiliza un contador de visitas con código malicioso

En una URL, utilizan un contador de visitas gratuito que está comprometido. Cuando accedes a la página, se ejecuta el contador, y al ejecutarse explota una vulnerabilidad (Neosploit) que infecta la máquina con un troyano. Con la reputación web activada, se corta el acceso al contador y con ello se corta la ejecución del contador, pero se puede acceder al resto del contenido de la página.